Action of Dihedral Groups

Ming-chang Kang

Department of Mathematics

National Taiwan University

Taipei, Taiwan

E-mail: kang@math.ntu.edu.tw

Abstract. Let K be any field and G be a finite group. Let G act on the rational function field $K(x_g:\ g \in G)$ by K-automorphisms defined by $g \cdot x_h = x_{gh}$ for any $g,\ h \in G$. Denote by $K(G)$ the fixed field $K(x_g:\ g \in G)^G$. Noether's problem asks whether $K(G)$ is rational (=purely transcendental) over K. We will give a brief survey of Noether's problem for abelian groups and dihedral groups, and will show that $\mathbb{Q}(D_n)$ is rational over $\mathbb{Q}$ for $n \leq 10$.

Mathematics Subject Classification 2000: Primary 12F12, 13A50, 11R32, 14E08.

Keywords: Noether's problem, rationality problem, dihedral groups.

This article was written for a local conference in 2005. It was circulated among a few friends, but has not been published ever since. It is not difficult to adapt the proof of this article so that the base field $\mathbb{Q}$ is replaced by a rather general field k.

§1. Introduction

Let K be any field and G be a finite group. Let G act on the rational function field $K(x_g:\ g\in G)$ by K-automorphisms such that $g\cdot x_h=x_{gh}$ for any $g,\ h\in G$. Denote by $K(G)$ the fixed field $K(x_g:\ g\in G)^G=\{f\in K(x_g:g\in G):\ \sigma\cdot f=f$ for any $\sigma\in G\}$. Noether's problem asks whether $K(G)$ is rational (=purely transcendental) over K [No].

Noether's problem arose from the study of the inverse Galois problem. In particular, if $K(G)$ is rational and K is an infinite field, then a generic polynomial for Galois G-extensions over K exists [DM; Sa1]. In case K is a Hilbertian field, i.e. Hilbert irreducibility theorem is valid for irreducible polynomials $f\in K[x_1,x_2,\cdots,x_n]$ (for example, an algebraic number field or a field K which is finitely generated over some field k so that trans $\deg_k K\geq 1$), the existence of a generic polynomial for Galois G-extensions over K will certainly guarantee an infinite family of Galois field extensions of K with Galois groups isomorphic to G.

The first solution of Noether's problem is provided by E. Fischer, a friend of Emmy Noether introducing to her the then novel and abstract thinking of Dedekind and Hilbert.

Theorem 1.1. (Fischer [Fi]) *Let G be a finite abelian group with exponent e and K be any field containing a primitive e-th root of unity. Then $K(G)$ is rational over K.*

On the other hand only a handful of results for the rationality of $\mathbb{Q}(G)$ were known before 1950's. Samson Breuer was able to show that $\mathbb{Q}(\mathbb{Z}_3)$ and $\mathbb{Q}(\mathbb{Z}_6)$ are rational over $\mathbb{Q}$ where $\mathbb{Z}_n$ is the cyclic group of order n [Br1]; he then showed that $\mathbb{Q}(G)$ is rational for some transitive solvable subgroup G contained in S_p, the symmetric group of degree p, if $p=5$ or 7 [Br2]. Breuer's results for transitive

solvable subgroups in S_p was extended by Furtwängler for $p = 5,\ 7,\ 11$ [Fr]; finally Breuer himself extended these results for any prime number $p \leq 23$ [Br3]. Several years later Gröbner proved that $\mathbb{Q}(G)$ is rational if G is the quaternion group of order 8 [Gr].

Unfortunately almost all these results, except Fischer's Theorem, were forgotten after World War II. In 1955 H. Kuniyoshi and K. Masuda resumed this problem ; they called it a problem of Chevalley. Masuda rediscovered many previous results; in particular he proved that $\mathbb{Q}(\mathbb{Z}_p)$ is rational if $p = 3,\ 5,\ 7,\ 11$ [Ma]. To the surprise of most people Swan constructed the first counter-example to Nother's problem in 1969 [Sw1]: $\mathbb{Q}(\mathbb{Z}_p)$ is not rational over $\mathbb{Q}$ if $p = 47,\ 113,\ 233, \cdots$. The reader is referred to the survey articles [Sw1; Sw2; Sa2; Ke; Ka2] for subsequent progress of Noether's problem. We will remark that Noether's problem for finite abelian groups has been solved completely [Le].

In the remaining of this article we will focus on the rationality of $\mathbb{Q}(D_n)$ where $D_n =< \sigma,\ \tau :\ \sigma^n = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} >$ is the dihedral group of order $2n$. As mentioned before, the rationality of $\mathbb{Q}(D_p)$ was proved for prime numbers $p \leq 23$ by S. Breuer and Furtwängler. It seems strange that the answer to the rationality of $\mathbb{Q}(D_n)$, $3 \leq n \leq 10$, is difficult to locate in the literature. The rationality of $\mathbb{Q}(D_8)$ can be found in [CHK, Theorem 3.1]; an easier case, the rationality of $\mathbb{Q}(D_4)$, is given in [CHK, Proposition 2.6]. In fact, $K(G)$ is rational for any field K and any non-abelian group G of order 8 or 16, except for the case when G is the generalized quaternion group of order 16 [CHK; Ka2]. The task of this article is to study the rationality problem of $\mathbb{Q}(D_6)$, $\mathbb{Q}(D_9)$ and $\mathbb{Q}(D_{10})$. What we will prove is the following.

Theorem 1.2. *$\mathbb{Q}(D_n)$ is rational over $\mathbb{Q}$ for $3 \leq n \leq 10$.*

Needless to say, the method in proving the above theorem may be adapted for a more general context, which will be embodied in a separate article. One of the purposes of this article is to illustrate some techniques of solving Noether's problem through concrete cases.

The article is organized as follows: Some basic tools will be recalled in Section 2. The rationality of $\mathbb{Q}(D_9)$ (resp. $\mathbb{Q}(D_6)$ and $\mathbb{Q}(D_{10})$) will be proved in Section 3 (resp. Section 4). The proof of Theorem 1.2 will be finished once we obtain Theorem 3.1, Theorem 4.1 and Theorem 4.2.

§2. Preliminaries

We recall some basic results which will be used in Section 3 and Section 4.

Theorem 2.1. ([CHK, Theorem 2.1]) *Let L be a field and G be a finite group acting on $L(x_1,\cdots,x_n)$, the rational function field of m variables over L. Suppose that*

(i) *for any $\sigma\in G$, $\sigma(L)\subset L$;*

(ii) *the restriction of the action of G on L is faithful;*

(iii) *for any $\sigma\in G$,*

$$\begin{pmatrix}\sigma(x_1)\\ \vdots\\ \sigma(x_m)\end{pmatrix}=A(\sigma)\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}+B(\sigma)$$

where $A(\sigma)\in GL_m(L)$ and $B(\sigma)$ is an $m\times 1$ matrix over L. Then there exists $z_1,\cdots,z_m\in L(x_1,\cdots,x_m)$ with $L(x_1,\cdots,x_m)=L(z_1,\cdots,z_m)$ such that $\sigma(z_i)=z_i$ for any $\sigma\in G$, any $1\le i\le m$.

Theorem 2.2. ([CHK, Theorem 2.4]) *Let G be any group whose order may be finite or infinite. Suppose that G acts on $L(x)$, the rational function field of one variable*

over a field L. Assume that, for any $\sigma \in G$, $\sigma(L) \subset L$, and $\sigma(x) = a_\sigma \cdot x + b_\sigma$ for some $a_\sigma, b_\sigma \in L$ with $a_\sigma \neq 0$. Then $L(x)^G$ is rational over L^G.

Theorem 2.3. ([CHK, Theorem 2.3]) *Let K be any field, $a,\ b \in K \setminus \{0\}$ and $\sigma : K(x,y) \longrightarrow K(x,y)$ be a K-automorphism defined by $\sigma(x) = a/x$, $\sigma(y) = b/y$. Then $K(x,y)^{<\sigma>} = K(u,v)$ where*

$$u = \frac{x - \dfrac{a}{x}}{xy - \dfrac{ab}{xy}}, \qquad v = \frac{y - \dfrac{b}{y}}{xy - \dfrac{ab}{xy}}.$$

Theorem 2.4. (Hajja [Ha]) *Let K be any field and G be a finite group. Suppose that G acts on the rational function field $K(x_1, x_2)$ by K-automorphisms such that, for any $\sigma \in G$, for $1 \leq i \leq 2$, $\sigma(x_i) = a_i(\sigma) \cdot x_1^{m_i(\sigma)} x_2^{n_i(\sigma)}$ where $a_i(\sigma) \in K \setminus \{0\}$ and $m_i(\sigma),\ n_i(\sigma) \in \mathbb{Z}$. Then $K(x_1, x_2)^G$ is rational over K.*

§3. $\mathbb{Q}(D_9)$

Let $D_n =< \sigma,\ \tau : \sigma^n = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} >$ be the dihedral group of order $2n$. Let $V = \bigoplus_{g \in D_n} \mathbb{Q} \cdot x(g)$ be the regular representation space of D_n over $\mathbb{Q}$, i.e. $g \cdot x(h) = x(gh)$ for any $g,\ h \in D_n$.

Define $x_i = x(\sigma^i) + x(\sigma^i \tau)$ for $0 \leq i \leq n-1$. Then

$$\sigma : x_0 \mapsto x_1 \mapsto \cdots \mapsto x_{n-1} \mapsto x_0,$$

$$\tau : x_i \mapsto x_{-i}$$

where the index of x_i is taken modulo n.

Clearly $\bigoplus_{0 \leq i \leq n-1} \mathbb{Q} \cdot x_i$ is a faithful D_n-subspace of V. By Theorem 2.1, if $\mathbb{Q}(x_0, \cdots, x_{n-1})^{D_n}$ is rational over $\mathbb{Q}$, then $\mathbb{Q}(D_n) = \mathbb{Q}(x_g : g \in D_n)^{D_n}$ is also rational over $\mathbb{Q}$.

We will prove that $\mathbb{Q}(x_0, \cdots, x_{n-1})^{D_n}$ is rational over $\mathbb{Q}$ for $n = 9, 6, 10$.

Theorem 3.1. $\mathbb{Q}(x_0, \cdots, x_8)^{D_9}$ *is rational over* $\mathbb{Q}$.

Proof. Step 1. Let ζ be a primitive 9-th root of unity and $\pi = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. Let $\rho \in \pi$ such that $\rho(\zeta) = \zeta^2$. Then ρ is a generator of π.

Extend the actions of D_9 and π to $\mathbb{Q}(\zeta)(x_0, \cdots, x_8)$ by requiring $\sigma(\zeta) = \tau(\zeta) = \zeta$, $\rho(x_i) = x_i$ for $0 \leq i \leq 8$.

Define $y_i = \sum_{0 \leq j \leq 8} \zeta^{-ij} x_j$. Then

$$\sigma : y_i \mapsto \zeta^i y_i,$$

$$\tau : y_i \mapsto y_{-i},$$

$$\rho : y_i \mapsto y_{2i}$$

We find that $\mathbb{Q}(x_0, \cdots, x_8)^{D_9} = \{\mathbb{Q}(\zeta)(x_0, \cdots, x_8)^{<\rho>}\}^{D_9} = \mathbb{Q}(\zeta)(x_0, \cdots, x_8)^{<D_9, \rho>} = \mathbb{Q}(\zeta)(y_0, \cdots, y_8)^{<\sigma,\tau,\rho>}$. Moreover $\tau \cdot \rho^3(y_i) = y_i$ for any $0 \leq i \leq 8$.

By Theorem 2.1, if $\mathbb{Q}(\zeta)(y_i : i \in \mathbb{Z}_9^\times)^{<\sigma,\tau,\rho>}$ is rational over $\mathbb{Q}$, so is $\mathbb{Q}(\zeta)(y_0, \cdots, y_8)^{<\sigma,\tau,\rho>}$. Hence it suffices to prove that $\mathbb{Q}(\zeta)(y_i : i \in \mathbb{Z}_9^\times)^{<\sigma,\tau,\rho>}$ is rational over $\mathbb{Q}$.

Step 2. Let $< y_1, y_2, y_4, y_5, y_7, y_8 >$ be the multiplicative subgroup of $\mathbb{Q}(\zeta)(y_0, \cdots, y_8) \setminus \{0\}$ generated by y_i where $i \in \mathbb{Z}_9^\times$. As an abelian group, the group $< y_1, y_2, y_4, y_5, y_7, y_8 >$ is isomorphic to the free abelian group $\mathbb{Z}^6$.

There is a natural π-module structure on $< y_1, y_2, y_4, y_5, y_7, y_8 >$. As a module over $\Lambda := \mathbb{Z}[\pi]$, $< y_1, y_2, y_4, y_5, y_7, y_8 >$ is isomorphic to Λ. In fact,we may identify y_1, y_2 with $1, \rho \in \Lambda$ respectively and write $\Lambda =< y_1, y_2, y_4, y_5, y_7, y_8 >$.

Define a map

$$\begin{aligned} \Phi : \Lambda =< y_1, y_2, y_4, y_5, y_7, y_8 > &\longrightarrow \mathbb{Z}_9 \\ y &\longmapsto \bar{j} \end{aligned}$$

if $\sigma(y) = \zeta^j y$ where $y = y_1^{a_1} y_2^{a_2} y_4^{a_4} y_5^{a_5} y_7^{a_7} y_8^{a_8}$ with $a_i \in \mathbb{Z}$.

Define a π-module structure on $\mathbb{Z}_9$ by $\rho \cdot \overline{j} = \overline{2j}$. Thus Φ becomes a π-equivariant map, i.e. $\Phi(\lambda \cdot y) = \lambda \cdot \Phi(y)$ for any $\lambda \in \pi$.

Let M be the kernel of Φ. Then $\mathbb{Q}(\zeta)(y_1, y_2, y_4, y_5, y_7, y_8)^{<\sigma>} = \mathbb{Q}(\zeta)(M)$. Note that M is an ideal of Λ with $[\Lambda : M] = 9$.

By [Le, (3.3) Proposition, p. 311], M is a projective Λ-module.

Step 3. We will prove that M is a free module over Λ. In fact, we will show that any rank-one Λ-projective module is free.

Write $\Lambda = \mathbb{Z}[T]/ < T^6 - 1 >$, $\Lambda_1 = \mathbb{Z}[T]/ < T^3 + 1 >$, $\Lambda_2 = \mathbb{Z}[T]/ < T^3 - 1 >$. (Note that $\Lambda_1 \simeq \Lambda_2$.) It is not difficult to prove that all the Picard groups of Λ, Λ_1, Λ_2 are zero by using Mayer-Vietoris sequences of K-groups [Mi, Theorem 3.3, p. 28] for the Cartesian squares

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_1 \\ \downarrow & & \downarrow \\ \Lambda_2 & \longrightarrow & \mathbb{Z}_2[T]/< T^3 - 1 > \end{array} \qquad \begin{array}{ccc} \Lambda_2 & \longrightarrow & \mathbb{Z}[\zeta_3] \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}_3 \end{array}$$

where ζ_3 is a primitive 3rd root of unity.

Step 4. By Step 3, we may find $z_0 \in < y_1, y_2, y_4, y_5, y_7, y_8 >$ such that $\mathbb{Q}(M) = \mathbb{Q}(z_0, z_1, \cdots, z_5)$where $z_i = \rho^i(z_0)$ for $1 \leq i \leq 5$. Clearly $\rho : z_0 \mapsto z_1 \mapsto z_2 \mapsto z_3 \mapsto z_4 \mapsto z_5 \mapsto z_0$ and $\tau\rho^3$ is the identity map on $\mathbb{Q}(z_0, \cdots, z_5)$.

Now $\mathbb{Q}(\zeta)(y_1, y_2, y_4, y_5, y_7, y_8)^{<\tau\rho^3>} = \mathbb{Q}(\zeta)(z_0, \cdots, z_5)^{<\tau\rho^3>} = \mathbb{Q}(\eta)(z_0, \cdots, z_5)$ where $\eta = \zeta + \zeta^{-1}$. It remains to show that $\mathbb{Q}(\eta)(z_0, \cdots, z_5)^{<\rho>}$ is rational.

Define $u_i = z_i - z_{i+3}$, $v_i = z_i + z_{i+3}$ for $0 \leq i \leq 2$. We find that

$$\rho : u_0 \mapsto u_1 \mapsto u_2 \mapsto -u_0, \quad v_0 \mapsto v_1 \mapsto v_2 \mapsto v_0.$$

By Theorem 2.1, it suffices to show that $\mathbb{Q}(\eta)(u_0, u_1, u_2)^{<\rho>}$ is rational over $\mathbb{Q}$.

Step 5. Note that $\rho^3(u_i) = -u_i$. Define $v_0 = u_0^2,\ v_1 = u_1/u_0,\ v_2 = u_2/u_1$. Then $\mathbb{Q}(\eta)(u_0, u_1, u_2)^{<\rho^3>} = \mathbb{Q}(\eta)(v_0, v_1, v_2)$. Moreover,

$$\rho : v_0 \mapsto v_0 v_1^2, \quad v_1 \mapsto v_2 \mapsto -1/(v_1 v_2).$$

By Theorem 2.1, if $\mathbb{Q}(\eta)(v_1, v_2)^{<\rho>}$ is rational over $\mathbb{Q}$, then $\mathbb{Q}(\eta)(v_0, v_1, v_2)^{<\rho>}$ is also rational over $\mathbb{Q}$.

Step 6. Define $w_1 = 1/(1 - v_1 + v_1 v_2),\ w_2 = -v_1/(1 - v_1 + v_1 v_2)$. Then $\mathbb{Q}(\eta)(v_1, v_2) = \mathbb{Q}(\eta)(w_1, w_2)$ and $\rho : w_1 \mapsto w_2 \mapsto -w_1 - w_2 + 1$. By Theorem 2.1, $\mathbb{Q}(\eta)(w_1, w_2) = \mathbb{Q}(\eta)(X, Y)$ for some $X,\ Y$ such that $\rho(X) = X,\ \rho(Y) = Y$. Hence $\mathbb{Q}(\eta)(w_1, w_2)^{<\rho>} = \mathbb{Q}(\eta)(X, Y)^{<\rho>} = \mathbb{Q}(\eta)^{<\rho>}(X, Y) = \mathbb{Q}(X, Y)$ $\square$

Remark. We may prove that $\mathbb{Q}(D_n)$ is rational when $n = 3,\ 5,\ 6,\ 7$ by the same method as above. For the case when $n = 6$, see Theorem 4.1 for another proof.

§4. $\mathbb{Q}(D_6)$ and $\mathbb{Q}(D_{10})$

We will prove that $\mathbb{Q}(x_0, \cdots, x_{n-1})^{D_n}$ is rational for $n = 6$, 10 where $\sigma : x_0 \mapsto x_1 \mapsto \cdots \mapsto x_{n-1} \mapsto x_0,\ \tau : x_i \mapsto x_{-i}$.

Let $n = 2m$ where m is an odd integer. (In case n =6, 10, m is actually an odd integer.) Define $y_i = x_i - x_{m+i},\ y_i' = x_i + x_{m+i}$ where $0 \le i \le m-1$. We get

$$\sigma : y_0 \mapsto y_1 \mapsto \cdots \mapsto y_{m-1} \mapsto -y_0, \quad y_0' \mapsto y_1' \mapsto \cdots \mapsto y_{m-1}' \mapsto y_0',$$

$$\tau : y_0 \mapsto y_0, \quad y_0' \mapsto y_0', \quad y_i \mapsto -y_{-i}, \quad y_i' \mapsto y_{-i}'$$

where the index of y_i is taken modulo m.

By Theorem 2.1, it suffices to prove the rationality of $\mathbb{Q}(y_0, \cdots, y_{m-1})^{D_n}$.

Theorem 4.1. *$\mathbb{Q}(y_0, y_1, y_2)^{D_6}$ is rational over $\mathbb{Q}$.*

Proof. Recall that $\sigma : y_0 \mapsto y_1 \mapsto y_2 \mapsto -y_0,\ \tau : y_0 \mapsto y_0,\ y_1 \mapsto -y_2,\ y_2 \mapsto -y_1$.

Define $z_1 = y_1/y_0,\ z_2 = y_2/y_1$. We find

$$\sigma : y_0 \mapsto y_0 z_1,\ z_1 \mapsto z_2 \mapsto -1/(z_1 z_2),$$

$$\tau : y_0 \mapsto y_0,\ z_1 \mapsto -z_1 z_2,\ z_2 \mapsto 1/z_2.$$

By Theorem 2.2, it suffices to prove that $\mathbb{Q}(z_1, z_2)$ is rational over $\mathbb{Q}$. But $\mathbb{Q}(z_1, z_2)^{<\sigma,\tau>}$ is rational by Theorem 2.4. $\square$

Theorem 4.2. *$\mathbb{Q}(y_0, \cdots, y_4)^{D_{10}}$ is rational over $\mathbb{Q}$.*

Proof. Recall that $\sigma : y_0 \mapsto y_1 \mapsto y_2 \mapsto y_3 \mapsto y_4 \mapsto -y_0,\ \tau : y_0 \mapsto y_0,\ y_1 \mapsto -y_4,\ y_2 \mapsto -y_3,\ y_3 \mapsto -y_2,\ y_4 \mapsto -y_1$.

Step 1. Let ζ be a primitive 5-th root of unity and $\pi = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. Let $\rho \in \pi$ such that $\rho(\zeta) = \zeta^2$. Then ρ is a generator of π.

Extend the actions of D_{10} and π to $\mathbb{Q}(\zeta)(y_0, \cdots, y_4)$ by requiring $\sigma(\zeta) = \tau(\zeta) = \zeta,\ \rho(y_i) = y_i$ for $0 \le i \le 4$. Note that $\mathbb{Q}(y_0, \cdots, y_4)^{<\sigma,\tau>} = \mathbb{Q}(\zeta)(y_0, \cdots, y_4)^{<\sigma,\tau,\rho>}$.

For $0 \le i \le 4$, define $z_i = \prod_{j \ne i}(\sigma + \zeta^j)(y_0)$. We find that

$$\sigma : z_i \mapsto -\zeta^i z_i,$$

$$\tau : z_i \mapsto \zeta^{-2i} z_{-i},$$

$$\rho : \zeta \mapsto \zeta^2,\ z_i \mapsto z_{2i}$$

where the index of z_i is taken modulo 5.

By Theorem 2.1, it suffices to prove that $\mathbb{Q}(\zeta)(z_1, z_2, z_3, z_4)^{<\sigma,\tau,\rho>}$ is rational over $\mathbb{Q}$.

Step 2. For $2 \le i \le 4$, define $u_i = z_i/z_{i-1}$. Then $\mathbb{Q}(\zeta)(z_1, z_2, z_3, z_4) = \mathbb{Q}(\zeta)(z_1, u_2, u_3, u_4)$ and

$$\sigma : z_1 \mapsto -\zeta z_1,\ u_i \mapsto \zeta u_i \quad \text{for } 2 \le i \le 4,$$

$$\tau : z_1 \mapsto \zeta^3 z_1 u_2 u_3 u_4,\ u_2 \mapsto \zeta^3/u_4,\ u_3 \mapsto \zeta^3/u_3,\ u_4 \mapsto \zeta^3/u_2,$$

$$\rho : z_1 \mapsto z_1 u_2,\ u_2 \mapsto u_3 u_4,\ u_3 \mapsto 1/(u_2 u_3 u_4),\ u_4 \mapsto u_2 u_3.$$

By Theorem 2.2, it suffices to prove that $\mathbb{Q}(\zeta)(u_2,u_3,u_4)^{<\sigma,\tau,\rho>}$ is rational over $\mathbb{Q}$.

Step 3. Define $v_1=u_2^5,\ v_2=u_4/u_2,\ v_3=u_3/u_2$. Then $\mathbb{Q}(\zeta)(u_2,u_3,u_4)^{<\sigma>}=\mathbb{Q}(\zeta)(v_1,v_2,v_3)$ and

$$\tau: v_1\mapsto 1/(v_1v_2^5),\ v_2\mapsto v_2,\ v_3\mapsto v_2/v_3,$$

$$\rho: v_1\mapsto v_1^2v_2^5v_3^5,\ v_2\mapsto 1/v_2,\ v_3\mapsto 1/(v_1v_2^2v_3^2).$$

Clearly $\mathbb{Q}(\zeta)(v_1,v_2,v_3)^{<\tau\rho^2>}=\mathbb{Q}(\eta)(v_1,v_2,v_3)$ where $\eta=\zeta+\zeta^{-1}$. Note that $\mathbb{Q}(\eta)=\mathbb{Q}(\sqrt{5})$. It remains to find $\mathbb{Q}(\sqrt{5})(v_1,v_2,v_3)^{<\rho>}$.

Step 4. Define $t=1/v_2,\ x=v_1v_2v_3^2,\ y=v_3$. Then $\mathbb{Q}(\sqrt{5})(v_1,v_2,v_3)=\mathbb{Q}(\sqrt{5})(t,x,y)$ and

$$\rho:\sqrt{5}\mapsto-\sqrt{5},\ t\mapsto 1/t,\ x\mapsto y\mapsto t/x\mapsto 1/(ty)\mapsto x,$$

$$\rho^2: t\mapsto t,\ x\mapsto t/x,\ y\mapsto 1/(ty).$$

Define

$$u=\frac{x-\dfrac{a}{x}}{xy-\dfrac{ab}{xy}},\qquad v=\frac{y-\dfrac{b}{y}}{xy-\dfrac{ab}{xy}}$$

where $a=t,\ b=1/t$. Apply Theorem 2.3. We get $\mathbb{Q}(\sqrt{5})(t,x,y)^{<\rho^2>}=\mathbb{Q}(\sqrt{5})(t,u,v)$.

Step 5. The action of ρ on $u,\ v$ is given by

$$\rho: u\mapsto\frac{y-\dfrac{b}{y}}{\dfrac{ay}{x}-\dfrac{bx}{y}},\qquad v\mapsto\frac{-(x-\dfrac{a}{x})}{\dfrac{ay}{x}-\dfrac{bx}{y}}.$$

Define $w=u/(tv)$. Then $\mathbb{Q}(\sqrt{5})(t,u,v)=\mathbb{Q}(\sqrt{5})(t,v,w)$ and

$$\rho:\sqrt{5}\mapsto-\sqrt{5},\ w\mapsto -1/w,\ v\mapsto\lambda/v$$

where $\lambda = 1/(w - (1/w))$ because

$$\frac{x - \dfrac{a}{x}}{\dfrac{ay}{x} - \dfrac{bx}{y}} = -\frac{u}{bu^2 - av^2}. \tag{1}$$

Note that the above identity is the identity (3) in [CHK, p. 156].

Define $s = \sqrt{5}(1+t)/(1-t)$. Then $\rho(s) = s$. Thus $\mathbb{Q}(\sqrt{5})(t,v,w)^{<\rho>} = \mathbb{Q}(\sqrt{5})(s,v,w)^{<\rho>} = \mathbb{Q}(\sqrt{5})(v,w)^{<\rho>}(s)$. It remains to prove that $\mathbb{Q}(\sqrt{5})(v,w)^{<\rho>}$ is rational over $\mathbb{Q}$.

Step 6. Let $\alpha = \sqrt{5} - 2$ and $\beta = 1/(w+1)$. Then $\alpha \cdot \rho(\alpha) = -1$ and $\beta \cdot \rho(\beta) = 1/(w - (1/w)) = \lambda$. Define $W = w/\alpha,\ V = v/\beta$. Then $\mathbb{Q}(\sqrt{5})(v,w) = \mathbb{Q}(\sqrt{5})(V,W)$ and $\rho(V) = 1/V,\ \rho(W) = 1/W$. Define $X = (1+V)/(1-V),\ Y = (1+W)/(1-W)$. Then $\mathbb{Q}(\sqrt{5})(V,W) = \mathbb{Q}(\sqrt{5})(X,Y)$ and $\rho(X) = -X,\ \rho(Y) = -Y$. Since $\rho(\sqrt{5}X) = \sqrt{5}X$ and $\rho(\sqrt{5}Y) = \sqrt{5}Y$, it follows that $\mathbb{Q}(\sqrt{5})(X,Y)^{<\rho>} = \mathbb{Q}(\sqrt{5})(\sqrt{5}X, \sqrt{5}Y)^{<\rho>} = \mathbb{Q}(\sqrt{5})^{<\rho>}(\sqrt{5}X, \sqrt{5}Y) = \mathbb{Q}(\sqrt{5}X, \sqrt{5}Y)$ is rational over $\mathbb{Q}$. $\square$

REFERENCES

[Br1] S. Breuer, *Zyklische Gleichungen 6. Grades und Minimalbasis*, Math. Ann. **86**(1922) 108-113.

[Br2] S. Breuer, *Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad*, Math. Ann. **92**(1924) 126-144.

[Br3] S. Breuer, *Metazyklischen Minimalbasis und komplexe Primzahlen*, J. reine angew. Math **156** (1927) 13-42.

[CHK] H. Chu, S. J. Hu and M. Kang, *Noether's problem for dihedral 2-groups*, Comment. Math. Helv. **79**(2004) 147-159.

[DM] F. DeMeyer and T. McKenzie, *On generic polynomials*, J. Algebra **261**(2003) 327-333.

[Fi] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen (1915) 77-80.

[Fu] P. Furtwängler, *Über Minimalbasen für Köper rationalen Funktionen*, S. -B. Akad. Wiss. Wien **134**(1925) 69-80.

[Gr] W. Gröbner, *Minimalbasis der Quaternionengruppe*, Monatshefte für Math. und Physik **41**(1934) 78-84.

[Ha] M. Hajja *Rationality of finite groups of monomial automorphisms of $K(X,Y)$*, J. Algebra **109**(1987) 46-51.

[Ka1] M. Kang *Introduction to Noether's problem for dihedral groups*, Algebra Colloquium **11**(2004) 71-78.

[Ka2] M. Kang, *Noether's problem for dihedral 2-groups II*, to appear in "Pacific J. Math.".

[Ke] I. Kersten, *Noether's proiblem and normalization*, Jber. Deutsch Math.-Verein. **100** (1999) 3-22.

[Le] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. math. **25**(1974) 299-325.

[Ma] K. Masuda, *Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariant*, J. Math. Soc. Japan **20** (1968) 223-232.

[Mi] J. Milnor, Introduction to algebraic K-theory, Princetion Univ. Press, 1971, Princeton.

[No] E. Noether, *Rationale Funktionenköper*, Jber. Deutsch. Math. -Verein. **22**(1913) 316-319.

[Sa1] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982) 250-283.

[Sa2] D. J. Saltman, *Groups acting on fields: Noether's problem*, Contemp. Math. **43** (1985) 267-277.

[Sw1] R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. math. **7** (1969) 148-158.

[Sw2] R. G. Swan, *Galois Theory*, in "Emmy Noether, a tribute to her life and work", Marcel Dekker, 1981, New York.

[Sw3] R. G. Swan, *Noether's problem in Galois Theory*, in "Emmy Noether in Bryn Mawr", Springer-Verlag, 1983, New York.